

§ 15.3

other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

(b) *Delegation*. The authority of the Secretary under this part may be further delegated within DOT.

§ 15.3 Terms used in this part.

In addition to the terms in § 15.3 of this chapter, the following terms apply in this part:

Administrator means the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee.

Coast Guard means the United States Coast Guard.

Covered person means any organization, entity, individual, or other person described in § 15.7. In the case of an individual, *covered person* includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. *Covered person* includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in § 15.7.

DHS means the Department of Homeland Security and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.

DOT means the Department of Transportation and any operating administration, entity, or office within the Department of Transportation, including the Saint Lawrence Seaway Development Corporation and the Bureau of Transportation Statistics.

Federal Flight Deck Officer means a pilot participating in the Federal Flight Deck Officer Program under 49 U.S.C. 44921 and implementing regulations.

49 CFR Subtitle A (10–1–15 Edition)

Maritime facility means any facility as defined in 33 CFR part 101.

Record includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term *record* also includes any draft, proposed, or recommended change to any record.

Security contingency plan means a plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management.

Security program means a program or plan and any amendments developed for the security of the following, including any comments, instructions, or implementing guidance:

- (1) An airport, aircraft, or aviation cargo operation;
- (2) A maritime facility, vessel, or port area; or
- (3) A transportation-related automated system or network for information processing, control, and communications.

Security screening means evaluating a person or property to determine whether either poses a threat to security.

SSI means sensitive security information, as described in § 15.5.

Threat image projection system means an evaluation tool that involves periodic presentation of fictional threat images to operators and is used in connection with x-ray or explosives detection systems equipment.

TSA means the Transportation Security Administration.

Vulnerability assessment means any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area, vessel, aircraft, train, commercial motor vehicle, or pipeline, or a transportation-related automated system or network, to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation,

or decommissioning phase. A *vulnerability assessment* may include proposed, recommended, or directed actions or countermeasures to address security concerns.

§ 15.5 Sensitive security information.

(a) *In general.* In accordance with 49 U.S.C. 40119(b)(1), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Secretary of DOT has determined would—

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person; or

(3) Be detrimental to transportation safety.

(b) *Information constituting SSI.* Except as otherwise provided in writing by the Secretary of DOT in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

(1) *Security programs and contingency plans.* Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including—

(i) Any aircraft operator or airport operator security program or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103; and

(iv) Any security incident response plan established under 46 U.S.C. 70104.

(2) *Security Directives.* Any Security Directive or order—

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, or other authority;

(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.* related to maritime security; or

(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) *Information Circulars.* Any notice issued by DHS or DOT regarding a

threat to aviation or maritime transportation, including any—

(i) Information Circular issued by TSA under 49 CFR 1542.303 or 1544.305, or other authority; and

(ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) *Performance specifications.* Any performance specification and any description of a test object or test procedure, for—

(i) Any device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and

(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

(5) *Vulnerability assessments.* Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) *Security inspection or investigative information.* (i) Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that